METHODS AND APPARATUS FOR SECURELY CONFIGURING A MACHINE IN A PRE-OPERATING SYSTEM ENVIRONMENT

ABSTRACT

Methods and apparatus for securely configuring a machine in a pre-operating system environment are disclosed. A server determines if configuration updates are available to be transmitted to various clients that are enabled to receive configuration updates in a pre-operating system environment. The server broadcasts a message indicating the availability of a configuration update and requests an attestation from each of the responding clients. The attestation may be a conventional attestation if the client is a managed client or the attestation may be a pseudo-anonymous attestation if the client is an independent client. The server verifies the authenticity of the attestation by querying a Trusted Third Party and transmits the configuration update after the client's identity has been verified. The client receives the configuration update, applies the update, and then continues its booting process.